Defence Research and Development Canada | Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

13 December 2013

DRDC-RDDC-2013-L7

Produced for/Distribution List: Public Safety Canada

Scientific Letter

Beyond territorial security

Introduction

Researchers from Defence Research and Development Canada's Centre for Security Science (CSS) provide analytical support to the Public Safety (PS) Canada-led All Hazards Risk Assessment (AHRA) initiative, and conduct periodic reviews of the methodology and tools in order to ensure the development of a robust and defensible product. The AHRA team at PS Canada receives comments on the federal AHRA methodology and process from key stakeholders during the implementation of the annual business cycle.[1]

This scientific letter (SL), which addresses feedback received from federal institutions, offers a critical reading of territorial security by assessing the extent to which it incorporates elements of sovereignty and security. According to the AHRA Methodology Guidelines: 2012-13, "Territorial security is a core responsibility of the GC (Government of Canada) and provides the conditions permitting the free movement of Canadians, people, and legitimate goods within the country and across borders. It represents the effective functioning and control of international borders, and provides for the safety and security of Canadians to go about their lives in an ordinary fashion."[2]

Although the territorial security impact category is theoretically inclusive of a broad range of threats and hazards to Canadian sovereignty, an increasing number of current and emerging threats and challenges cannot be properly understood or assessed through the narrow, largely geographic prism of territorial security as it is currently expressed in the AHRA methodology. In fact, some of these threats and challenges may have little, if any, impact on the country's territorial integrity at all. This paper highlights several emerging trends in the strategic environment that present both a conceptual and, by extension, a methodological challenge to the existing AHRA framework in this regard.

Sovereignty and Territoriality

Although sovereignty and territoriality are closely related in practice, they are not actually coterminous. As Stephen Krasner explains,

> "The term sovereignty has been used in four different ways – international legal sovereignty, Westphalian sovereignty, domestic sovereignty, and interdependence sovereignty. International legal sovereignty refers to the practices associated with mutual recognition, usually between territorial entities that have formal juridical independence. Westphalian sovereignty refers to political organization based on the exclusion of external actors from authority structures within a given territory. Domestic sovereignty refers to the formal organization of political authority within the state and the ability of public authorities to exercise effective control within the borders of their own polity. Finally, interdependence sovereignty refers to the ability of public authorities to regulate the flow of information, ideas, goods, people, pollutants, or capital across the borders of their state."[3]

[1] Canada, Public Safety Canada, *All Hazards Risk Assessment Methodology Guidelines, 2012-13* (Ottawa: Public Safety Canada, Emergency Management Planning Division, 2013), pp. 7-8.
[2] Ibid., p. 39.
[3] Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, N.J.: Princeton University Press, 1999), pp. 3-4.

The question of territorial security thus comprises only a portion of the sovereignty landscape, which extends to the question of international recognition and acceptance of a state's ability to assert sovereignty. Legitimate control and jurisdictional authority are not necessarily derivative of physical control. In neglecting this critical dimension of sovereignty, the AHRA risks overlooking or undervaluing several emerging threats and challenges to Canada's sovereignty that do not neatly fit within the narrow parameters of the territorial security impact category. The following sections examine the differences between territorial security and sovereignty and how several emerging trends are likely to make these distinctions problematic.

Discussion

Climate Change

Climate change poses a unique challenge to Canadian sovereignty. Until recently, Canada's assertion of sovereignty in the North largely went unchallenged due to the region's remoteness and inaccessibility.[4] With climate change and the rapid decline in sea ice, however, challenges to Canadian sovereignty are likely to become much more pronounced and frequent. Even in the absence of direct territorial infringement, Canada may find its assertions of sovereignty in the Arctic increasingly contested by other states.[5]

Maritime Threats and Challenges

The maritime environment is an even more significant example of the limitations of territorial security as a framing concept. Events such as illegal migration or human smuggling underscore the importance of maritime surveillance and maritime domain awareness capabilities. Yet actions by vessels of interest, while still achieving impacts on Canadian sovereignty, may never actually generate a 'trigger' causing a distinct geographic impact on territorial security. Even a regular maritime incursion into Canadian territorial waters would not register any territorial security impact as it is currently measured.

The maritime environment in particular requires an entirely different approach to assessing territorial security and sovereignty in order to take into account a more expansive set of security problems, including transnational crime, human smuggling, piracy, unauthorized submarine transits, and terrorism. According to Peter Chalk, "The maritime realm is especially conducive to these types of threat contingencies given its vast, largely unregulated, and opaque nature."[6] The presence of strategic energy resources such as oil, gas, and minerals has the potential to create additional implications for the continuous monitoring, surveillance, and threat management of Canada's maritime approaches. In these cases, which do not fit our conventional understanding of territorial security, Canadian sovereignty will nevertheless be undermined before any impact on the country's territorial security is presented.

Cyberspace

Cyber threats to critical infrastructure (CI) and other computerized and networked systems, both governmental and private, present another set of challenges to territorial security as currently defined in the AHRA Methodology

[4] For more discussion on defining and asserting sovereignty in the Arctic, including international legal sovereignty, consult: Matthew Carnaghan and Allison Goody, "Canadian Arctic Sovereignty," Political and Social Division, Parliamentary Information and Research Service, 26 January 2006, pp. 2-4. http://www.parl.gc.ca/Content/LOP/researchpublications/prb0561-e.pdf.
[5] For discussion, see Ron Huebert, "Canadian Arctic Sovereignty and Security in a Transforming Circumpolar World," Foreign Policy for Canada's Tomorrow No. 4, Canadian International Council (July 2009), pp. 10-12. Available at: http://opencanada.org/wp-content/uploads/2011/05/Canadian-Arctic-Sovereignty-and-Security-Rob-Huebert1.pdf.
[6] Peter Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States* (Santa Monica, CA: RAND Corporation, 2008), p. iii.

Guidelines. Complicating this situation, the threat emanates from a wide range of actors: individuals, foreign governments, terrorist organizations, organized criminal networks, and other motivated actors.[7]

By its very nature, cyberspace functions differently than other environments. As a recent report notes, "minor players can exercise considerable power in the cyber domain, which has become a multi-dimensional attack space that enables perpetrators to target critical infrastructures remotely and without physical exposure to defensive forces. Traditional physical methods of protecting critical infrastructure are no longer sufficient, and Canada cannot continue to abide by the kind of reactive, defensive stance that has long characterized protective security."[8] The Iranian and Anonymous attacks are illustative of the strategic reality that actors lacking military capability to engage an adversary may employ novel techniques and tactics in ways that obsure the traditional domestic-international divide.[9] In this sense, cyber is a domain that is particularly well-suited to an adversary's capacity to wage an asymmetric attack in a manner that undermines geographic boundaries.

The challenge for Canada is that the government could find itself in a situation where some aspect of Canada's CI sector is compromised, leading to doubts about the government's ability to manage its own national critical infrastructure. The repeated penetration of Canadian networks and information systems would likely raise suspicions that Canada has become a security liability, particularly if American CI assets were affected or shut down via Canadian weaknesses in cyberspace. These technological developments, especially in regards to cloud computing, could have implications for cross-border data sharing and management issues as they relate to security and state sovereignty.[10]

Conclusion

As the examples discussed in this SL illustrate, sovereignty is a much broader concept than territorial security. A series of emerging threats and challenges is likely to make that distinction even starker as Canadian sovereignty is increasingly challenged by developments that have no territorial security dimension whatsoever. Given the shortcomings associated with the current definition of territorial security, the impact criteria in the AHRA Methodology Guidelines should be reviewed and modified accordingly.

---

[7] Activist hackers or 'hacktivists' are becoming increasingly more aggressive in pursuing illegal cyber threat activities, such as distributed denial of service (DDoS) and digital protest attacks, for criminal gain or to advance political/ideologically-inspired agendas. See Royal Canadian Mounted Police, "Hacktivism," Criminal Intelligence Brief, October 2012, p. 3.

[8] Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure," Report Prepared For The Canadian Security Intelligence Service, March 2012. http://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp#d. Accessed March 2013.

[9] For background on the Stuxnet virus see William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011. Accessed online at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0, 6 June 2013; and David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012. Accessed online at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, 6 June 2013. For commentary on the Anonymous attacks, consult: John D. Sutter, "Anonymous Declares 'Cyberwar' on Israel," CNN, 20 November 2012. Accessed online at http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/, 1 February 2013. Zack Colman, "Hacker Group Anonymous Plans Attack on Oil-and-Gas Industry," *The Hill*, 16 May 2013. Accessed online at http://thehill.com/blogs/e2-wire/e2-wire/300239-hacker-group-anonymous-plans-attack-on-oil-and-gas-industry, 6 June 2013.

[10] For discussion, see Ron Deibert, *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* (Calgary: Canadian Defence and Foreign Affairs Institute, August 2012), pp. 5-6.

References

Broad, William J., John Markoff, and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, 15 January 2011. Accessed online at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0, 6 June 2013.

Canada, Public Safety Canada, *All Hazards Risk Assessment Methodology Guidelines, 2011-12* (Ottawa: Public Safety Canada, Emergency Management Planning Division, 2012).

Carnaghan, Matthew and Allison Goody, “Canadian Arctic Sovereignty,” Political and Social Division, Parliamentary Information and Research Service, 26 January 2006, pp. 2-4. http://www.parl.gc.ca/Content/LOP/researchpublications/prb0561-e.pdf.

Chalk, Peter, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States* (Santa Monica, CA: RAND Corporation, 2008).

Colman, Zack, “Hacker Group Anonymous Plans Attack on Oil-and-Gas Industry,” *The Hill*, 16 May 2013. Accessed online at http://thehill.com/blogs/e2-wire/e2-wire/300239-hacker-group-anonymous-plans-attack-on-oil-and-gas-industry, 6 June 2013.

Gendron, Angela and Martin Rudner, “Assessing Cyber Threats To Canadian Infrastructure,” Report Prepared For The Canadian Security Intelligence Service, March 2012. http://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp#d. Accessed March 2013.

Huebert, Ron, “Canadian Arctic Sovereignty and Security in a Transforming Circumpolar World,” Foreign Policy for Canada’s Tomorrow No. 4, Canadian International Council (July 2009). Available at: http://opencanada.org/wp-content/uploads/2011/05/Canadian-Arctic-Sovereignty-and-Security-Rob-Huebert1.pdf.

Krasner, Stephen D., *Sovereignty: Organized Hypocrisy* (Princeton, N.J.: Princeton University Press, 1999).
Royal Canadian Mounted Police, “Hacktivism,” Criminal Intelligence Brief, October 2012.

Sanger, David E., “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*, 1 June 2012. Accessed online at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, 6 June 2013.

Sutter, John D., “Anonymous Declares ‘Cyberwar’ on Israel,” CNN, 20 November 2012. Accessed online at http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/, 1 February 2013.

Produced by: Friesen, Shaye and Greene, Brian

Canada